NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

The Anti-Terrorism Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

QUICK LINKS

North Dakota

Regional

National

International

Banking and Finance Industry

Chemical and Hazardous Materials Sector

Commercial Facilities

Communications Sector

Critical Manufacturing

Defense Industrial Base Sector

Emergency Services

Energy

Food and Agriculture

Government Sector (including Schools and Universities)

Information Technology and Telecommunications

Public Health

Transportation

Water and Dams

North Dakota Homeland Security Contacts

NORTH DAKOTA

(North Dakota) Firm hasn't paid North Dakota fine for wastewater violation. It's been two years since state regulators touted a record $1.5 million fine against a company for illegally dumping 20,000 barrels of toxic liquid and threatening drinking water supplies near a large western North Dakota city, and little has changed. The now-dissolved company is under federal investigation, the penalty is unpaid and the affected site is still contaminated.
http://rapidcityjournal.com/news/local/firm-hasn-t-paid-north-dakota-fine-for-wastewater-violation/article_481ea964-f57d-53ff-8eaf-7563f7b356eb.html

(North Dakota) North Dakota Department of Health Spreads Education About Ebola. North Dakota Department of Health officials say it's important that everyone is educated about ebola, no matter how far away it is. That's why the Health Department is partnering with public health units and health care professionals across the state to help spread awareness.
http://www.kxnet.com/story/26228200/north-dakota-department-of-health-spreads-education-about-ebola

(North Dakota) Oil Industry Funded Study Shows Bakken Crude is not More Volatile or Flammable. Final results on an industry funded study of Bakken crude says it's similar to other light sweet crude oils produced in the U.S. and is not more dangerous.The North Dakota Petroleum Council commissioned the study done by Turner, Mason & Company. http://www.kxnet.com/story/26193808/oil-industry-funded-study-shows-bakken-crude-is-not-more-volatile-or-flammable?autoStart=true&topVideoCatNo=default&clipId=10438298

REGIONAL

(Minnesota) 20,000 gallons of sewage spills into Rum River. A backed-up 14-inch sewer main at the under construction Cambridge Wastewater Treatment Facility in Minnesota caused an estimated 20,000 gallons of raw sewage to spill into the Rum River August 4. The plant ordered a replacement of temporary sewage pumps which appeared to clear the clog and fix the issue.
http://www.kare11.com/story/news/local/2014/08/05/20000-gallons-of-sewage-spills-into-rum-river/13623001/

(Wisconsin) Manure digester explosion sparks fire. Officials believe an explosion that destroyed the $250,000 nylon inflatable roof of a 1.25-million gallon manure digester at the Clear Horizons LLC biodigester near Waunakee was caused by the ignition of methane gas when an employee started an electric blower. The digester was taken offline indefinitely while authorities investigate and determine if the biodigester is safe to resume operations.
http://www.twincities.com/localnews/ci_26296885/manure-digester-explosion-sparks-fire

NATIONAL

(National) CDC issues highest-level alert for Ebola. The U.S. Centers for Disease Control and Prevention has issued its highest-level alert for a response to the Ebola crisis in West Africa. "Ops Center moved to Level 1 response to given the extension to Nigeria & potential to affect many lives," CDC chief Tom Frieden said Wednesday on Twitter.
http://www.usatoday.com/story/news/world/2014/08/06/ebola-nigeria-saudi-arabia-virus-death-toll/13663973/

(National) U.S. Homeland Security contractor reports computer breach. DHS and the U.S. Office of Personnel Management (OPM) suspended work with Virginia-based US Investigations Services (USIS) after the contractor reported a cyberattack likely involving the theft of personal information of DHS employees. DHS notified its entire workforce and is working with OPM, FBI, and USIS to determine the scope of the intrusion.
http://www.reuters.com/article/2014/08/07/us-usa-security-contractor-idUSKBN0G62N420140807

(National) Leaked CBP Report Shows Entire World Exploiting Open US Border. A leaked intelligence analysis from the Customs and Border Protection (CBP) reveals the exact numbers of illegal immigrants entering and attempting to enter the U.S. from more than 75 different countries.   http://www.breitbart.com/Breitbart-Texas/2014/08/03/Leaked-CBP-Report-Shows-Entire-World-Exploiting-Open-US-Border

International

(International) 1.2 billion unique credentials, 500 million email addresses stolen by Russian cyber gang. Researchers with Hold Security found that a Russian cybercrime group dubbed "CyberVor" was able to collect 1.2 billion unique credentials from the Web sites of a wide variety of large and small businesses, as well as over 500 million email address credentials. The researchers reported that the cybercriminals used SQL injection attacks and later botnets that scanned sites on a large scale looking for SQL vulnerabilities to obtain the information. http://news.softpedia.com/news/1-2-Billion-Unique-Credentials-500-Million-Email-Addresses-Stolen-by-Russian-Cyber-Gang-453677.shtml

(International) Attackers used multiple zero-days to hit spy agencies in cyber-espionage campaign. Kaspersky Lab researchers identified the infection methods used in the Epic Turla cyber-espionage campaign (also known as Snake or Uroburos) that targeted intelligence agencies, military organizations, government agencies, education institutions, pharmaceutical companies, and research groups in over 45 countries. The attackers behind the campaign used several malware platforms and zero-day exploits in Windows XP and Server 2003 and Adobe Reader to infect systems and then could upgrade the malware with additional capabilities once in place. http://www.securityweek.com/attackers-used-multiple-zero-days-hit-spy-agencies-cyber-espionage-campaign

(International) U.S. airstrikes bring early gains in Iraq. A series of U.S. airstrikes Sunday against militants in Iraq appeared to back up President Obama's promise of targeted attacks that could continue for months. http://www.usatoday.com/story/news/world/2014/08/10/more-air-strikes-in-iraq/13860607/

(Cuba) US sent Latin youth undercover in anti-Cuba ploy. Over at least two years, the U.S. Agency for International Development — best known for overseeing billions of dollars in U.S. humanitarian aid — sent nearly a dozen neophytes from Venezuela, Costa Rica and Peru to gin up opposition in Cuba. http://bigstory.ap.org/article/us-sent-latin-youth-undercover-anti-cuba-ploy

Banking and Finance Industry

(International) **U.S. charges 13 with spreading $77 million in fake bills.** Thirteen suspects arrested by U.S. Secret Service agents in May and June were indicted in federal court August 7 for allegedly operating a major counterfeit currency ring that distributed over $77 million in fake bills in several States along the East Coast since at least 1999. The fake bills were believed to have been manufactured in Israel, and the group allegedly established a counterfeit bill printing press in New Jersey in January 2014. http://www.businessweek.com/news/2014-08-07/u-dot-s-dot-charges-13-with-spreading-77-million-in-fake-bills

Chemical and Hazardous Materials Sector

Nothing Significant to Report

Commercial Facilities

Nothing Significant to Report

Communications Sector

Nothing Significant to Report

Critical Manufacturing

(International) **Car hacking enters remote exploitation phase.** Researchers at the Black Hat 2014 conference presented findings that showed how attackers could remotely compromise the systems of certain vehicles that integrate Bluetooth, radio, or other communications methods into their sensors and controls. Among the most vulnerable types of systems the researchers found were systems that can control vehicles automatically, such as active lane control, self-parking, and pre-collision systems. http://threatpost.com/car-hacking-enters-remote-exploitation-phase

Defense/ Industry Base Sector

Nothing Significant to Report

Emergency Services

(California) Thousands of gallons of water stolen from small town's fire department. Officials are investigating after thieves stole 8,000 gallons of water from the North San Juan Fire District in Nevada County by driving up to the valve and pumping water out of the water tanks on site.
http://sacramento.cbslocal.com/2014/08/07/thousands-of-gallons-of-water-stolen-from-small-towns-fire-department/

Energy

(Mississippi) Mississippi Power going coal-free at Plant Watson. The remaining two coal-fired units at Mississippi Power's Plant Watson in Gulfport will be converted to natural gas by April 2015 as part of a settlement between the company and the Sierra Club which will ensure the company is in compliance with new federal environmental standards. The settlement also includes establishing and funding a $15 million grant for an energy efficiency and renewable energy program associated with the Kemper County energy facility.
http://www.wlox.com/story/26190738/mississippi-power-going-coal-free-at-plant-watson

(Pennsylvania) State: Fracking waste tainted groundwater, soil at three Washington County sites. The Pennsylvania Department of Environmental Protection issued a violation notice to one Range Resources-owned impoundment site in Washington County and is increasing monitoring and testing at another site after leaks of fracking waste water were found at three impoundment sites which have contaminated soil and groundwater. Officials notified residents of their findings and assured the public that there was no potential contamination.
http://www.post-gazette.com/local/washington/2014/08/06/Pa-finds-tainted-water-soil-at-three-Washington-County-shale-sites/stories/201408050198

Food and Agriculture

(South Dakota, North Dakota) SD, ND have confirmed animal anthrax cases. SD State Vet says the disease is not a food safety concern, but more of an occupational concern. Anthrax bacteria spores lie dormant in the ground and can

become active under extreme weather like flooding and drought. Outbreaks can kill many animals quickly. An outbreak in North Dakota in 2005 killed more than 1,000 animals. http://bismarcktribune.com/news/state-and-regional/south-dakota-north-dakota-have-confirmed-animal-anthrax-cases/article_7af12f0e-1c04-11e4-8411-001a4bcf887a.html

Government Sector (including Schools and Universities)

Nothing Significant to Report

Information Technology and Telecommunications

(International) Registry-residing malware creates no file for antivirus to scan. A researcher with GData published details of a new type of malware dubbed Poweliks that can avoid detection by antivirus programs by not creating any file on the disk, performing its functions instead in the system memory, and making the registry key unavailable to the Registry Editor. http://news.softpedia.com/news/Registry-Residing-Malware-Creates-No-File-for-Antivirus-To-Scan-453374.shtml

(International) Synology NAS users hit with Cryptolocker variant. Users of Synology's network-attached storage (NAS) devices reported having devices infected with a variant of the Cryptolocker ransomware beginning over the weekend of August 2 that encrypts files and demands a ransom to decrypt them. The method by which the malware is infecting NAS devices is currently unknown and users were advised to backup their files and unplug the devices until the infection vector is identified. http://www.net-security.org/malware_news.php?id=2827

(International) Cracker takes control of 200 rooms in Chinese hotel. A security consultant revealed during the Black Hat 2014 conference that he was able to remotely control amenities in over 200 rooms at a luxury hotel in China due to an insecure automation protocol that is commonly used in China and Europe. Prior to the conference, the researcher alerted the hotel's parent company and the system flaw was corrected.

http://www.theregister.co.uk/2014/08/07/cracker_takes_control_of_200_rooms_in_chinese_hotel/

Public Health

Nothing Significant to Report

Transportation

(International) TSA checkpoint systems found exposed on the net. A Qualys researcher discovered two devices, the Morpho Detection Itemiser 3 and the Kronos 4500, used at U.S. airports and other security checkpoints have backdoors in which hackers can access usernames and passwords to the devices. The researchers also found about 6,000 Kronos time clock systems that are online and open to the public, two of which are located at U.S. airports.
http://www.darkreading.com/vulnerabilities---threats/advanced-threats/tsa-checkpoint-systems-found-exposed-on-the-net/d/d-id/1297843

Water and Dams

(Ohio; Michigan) 'Our water is safe,' Toledo mayor says in lifting ban. The mayor of Toledo, Ohio, lifted a tap water ban affecting as many as 400,000 people in Toledo and four municipalities in Michigan August 4 after test results returned nondetectable levels of an algae-related toxin. The tap water ban went into effect August 1 after the microcystin toxin was found in Lake Erie due to a harmful algae bloom. http://www.cnn.com/2014/08/04/us/toledo-water-warning/index.html

(Oregon; Washington) Corps of Engineers agrees to disclose dams' pollution. The U.S. Army Corps of Engineers announced August 4 that it will disclose the amount of pollutants being released into waterways among 8 dams on the Columbia and Snake rivers in Oregon and Washington as well as apply to the U.S. Environmental Protection Agency for pollution permits to settle Columbia Riverkeeper claims that they violated the Clean Water Act. The Corps did not admit any wrongdoing and will pay $143,000 in fees.
http://registerguard.com/rg/news/local/31967790-75/corps-of-engineers-agreesto-disclose-dams-pollution.html.csp

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455;   US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165